2008-06

Security Risk Management: Implementing a National Framework for Success in the Post 9-11 World

Jopeck, Edward

Security Risk Management: Implementing a National Framework for Success in the Post 9-11 World

Edward J. Jopeck, President
Security Analysis and Risk Management Association

Kerry L. Thomas, Executive Vice President
Security Analysis and Risk Management Association

Over the past several decades, significant resources have been expended by Federal departments and agencies to implement more uniform and rigorous security risk management processes and methods. However, despite the considerable sums spent to affect change, security risk management efforts across the Federal government have remained at roughly the same level in terms of sophistication, coordination and comparability as they were more than a decade ago. Furthermore, while some of these efforts have sought to dictate "standards" for government-wide use, none have gained significant acceptance outside of the organizations where they originated.

The terrorist attacks of September 11, 2001, and the subsequent creation of the Department of Homeland Security (DHS), have added a further degree of complexity to this issue. In addition to large numbers of new security risk analysis users, the focus on homeland security that emerged in the wake of these attacks also imbued security risk management efforts with significant sums of new money. DHS and other Federal agencies have used the new funding to develop and implement a variety of security programs, many of which rely on risk management principles as a key part of their decision framework. Despite this, the numerous directives and plans arising out of the homeland security enterprise either disseminate conflicting guidance or remain silent on risk management methods that should be employed to achieve comparable results. As a result, more than six years after 9/11, the Nation has not yet achieved a consistent, risk-based approach that provides decision-makers at all levels measurable results for intelligently reducing terrorist risks.

In the post 9/11 security environment, where the price of failure in both lives and dollars can be staggering, few can argue about the role of risk management or the urgency of overcoming the challenges to using it effectively. Just as the 9/11 Commission identified emergency responder radio interoperability as a critical shortfall, clear guidance on "interoperable" risk analysis approaches is also needed to permit effective risk communication between homeland security organizations with similar missions. This article attempts to identify the primary reasons for this apparent lack of progress, and explores a vision for implementing a more successful risk management program that can provide the Nation the security it needs at a price it can afford.

Identifying the Problems

While there is virtually no disagreement over the need to use risk as a decision support tool for homeland security activities, prior attempts to do so have failed largely because they did not address the fundamental building blocks needed to establish the basis for success. Figure 1 below illustrates this in more detail.

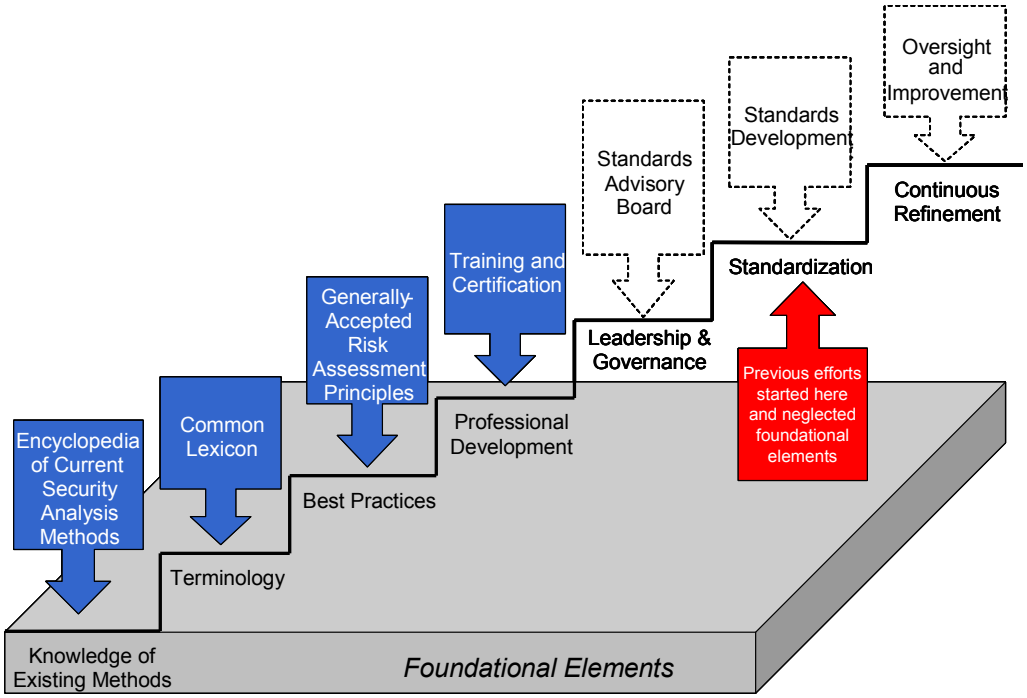

Figure 1.Creating the Foundation of Security Risk Management - The Building Blocks of Success

The underlying reasons for this trend are complex and bear further discussion:

- **Security risk management is an immature discipline that has developed independently and unevenly across the Federal Government and private industry**. DHS leadership correctly seized on the applicability of security risk analysis to the mandate of protecting the homeland, but it failed to ensure the processes and cadre of experienced risk analysts necessary to effectively serve the mission were in place. As such, there is still no system of standardized professional development to attract and educate the number of risk management practitioners the homeland security mission requires.

- **There is no national system of governance available to risk practitioners for collaborating on building interoperability into their risk management approaches.** Lacking an interagency advisory board or recognized standard-setting body, there is no way to synchronize divergent methods, arbitrate disputes or resolve crosscutting issues. Consequently, security risk practitioners often develop new methodologies rather than adopt, or adapt, an existing approach that doesn't fit their needs exactly. Furthermore, because the underlying methods are not based on recognized or compatible metrics,

the resulting data is often useless to other agencies that must then collect similar data using another methodology.

- **There is no comprehensive, documented body of knowledge on the current state of the security risk management discipline.** There is no encyclopedic reference to which practitioners may refer when considering how to best meet their security risk analysis needs. Without this body of knowledge, there is no way to determine where adequate methods already exist, decide where to focus additional research and development or ensure existing efforts are not duplicative and wasteful. Moreover, without this collection of knowledge, it will be difficult to train the next generation of security risk analysts and managers in a consistent manner.

- **The lack of a common professional language for security analysis and risk management divides practitioners and makes collaboration difficult.** This "language deficit" serves as a fundamental impediment to a cooperative approach on security risk analysis by the Government and the private sector. While many attempts to dictate standards within individual Federal departments and agencies have been attempted, their conflict with similar efforts elsewhere only exacerbates the problem. Without a common language to be used by practitioners when describing methods and needed improvements, future progress will remain frustratingly slow.

- **Looking to the future, there is currently no capability to train or certify the knowledge of security risk management professionals.** Given the huge investments being made in homeland security, coupled with the central role of risk management, it would seem logical that training and certification of current and future practitioners is a national requirement. Unfortunately, there is currently no recognized approach to risk management training for practitioners in Federal, state, and local government agencies, or in the private sector. Absent this, it is difficult to imagine that risk management will ever be done with accuracy, reliability or consistency.

Discussion

"The need for and difficulties associated with creating a coordinated, coherent risk management approach to the nation's homeland security have been widely acknowledged since the events of September 11, 2001, and the creation of DHS. Yet, this general acknowledgment has not been accompanied by the guidance necessary to make consistent use of risk management across DHS."

U.S. Government Accountability Office
Applying Risk Management Principles to Guide Federal Investments, GAO-O7-386T

Without the leadership and guidance necessary to overcome the noted challenges to applying security risk management processes and methods in a consistent manner, an intensely competitive environment between Federal departments and agencies, the contractors who support them, the National Labs, and academia has developed. The resulting free-for-all has slowed progress on this issue to a virtual standstill.

As long as each Federal department and agency stands alone, synchronization of methods and the ability to validate the conclusions of the resulting assessments is not possible. The net effect is that, since 2001, over $12 billion[1] has been distributed to state and local governments by DHS based on assessments of risk that do not provide any means to quantify the overall impact of the funds and that do not meet any recognized standard. Moreover, the almost annual changes to the process for allocating funding has prevented any sort of baseline from emerging and makes it virtually impossible to know if, in fact, the Nation is any safer now than before 2001.

Recognizing the need for a constructive forum to collaborate, improve professional methods and share information in a non-threatening environment, security practitioners have begun to take matters into their own hands. For example, the Security Analysis and Risk Management Association (SARMA) was formed in 2005 to help promote a balanced, cooperative approach to advancing security analysis methods and the profession in general. Likewise, the American Society for Industrial Security (ASIS) has begun developing its own risk management standard to fill the void in Federal security efforts. Even international organizations, such as the Risk Management Institute of Australasia, have stepped in to fill the void with an effort to document a common body of knowledge for security risk management. As such grass-roots movements gain momentum, the Federal government risks slipping still further behind in shaping the future of security risk management.

This problem is not insurmountable, however. In fact, a similar problem has been successfully addressed before. In 1988, then President Ronald Reagan issued National Security Decision Directive (NSDD) 298, which created a National Operations Security (OPSEC) Program in order to coordinate the efforts of all Federal departments and agencies with national security missions. Among other things, NSDD 298 created the Interagency OPSEC Support Staff (IOSS) to help promote sound methods and educate current and future generations in the use of the OPSEC methodology. Concerned practitioners also joined their efforts with those of the IOSS by creating the OPSEC Professionals Society to further the application of OPSEC as a professional discipline and foster high standards of professionalism and competence among practitioners.

A Path Forward

The urgent need for improved security risk management processes and consistent implementation across the Federal government requires strong leadership, a bold vision for coordinated governance, and a comprehensive plan to implement the partnerships necessary for a ***national strategy*** on security risk management. The past two decades have shown that the “every agency for itself” approach will not result in a coordinated national approach, as doing so is beyond the mission and authority of any one Federal department or agency. The Government Accountability Office (GAO) and Congressional Research Service (CRS) have both come to recognize this may be the case. In a December, 2005, report on homeland security risk management, GAO concluded:

[1] Congressional Research Service, The Department of Homeland Security’s Risk Assessment Methodology: Evolution, Issues, and Options for Congress, Order Code RL33858, Feb. 2, 2007, available at http://www.fas.org/sgp/crs/homesec/RL33858.pdf, accessed Sept.25, 2007

"For the results of a risk management system to be meaningful and useful, all related agencies should be using similar methods. If agencies' methods are not compatible, then comparisons between agencies become difficult and sector or national risk assessments becomes less reliable."[2]

CRS went further in detailing the importance not only of an interagency approach, but a National one that necessitates partnerships with those outside of the Federal government:

"A cohesive risk strategy and agreement on core terms amongst disparate agencies is desirable because many aspects of the risk management process are dependent on functions performed by agencies outside of the department. However, the necessity of common definitions and standards goes beyond the federal government. As states and localities continue to provide information to be included in the risk assessment process, to include, information on critical infrastructure sites within their respective jurisdictions and, eventually, investigative information, the rational for attempting to develop national-wide risk assessment strategy at all levels of government becomes stronger."[3]

We end this subsection by proposing a framework for decision makers to consider regarding the governance required to improve risk management nationally. The authors believe the essential elements of such a framework would include:

Leadership

Resolution of the interagency leadership problem requires a clear mandate from the White House to overcome the existing challenges. Steps that should be taken include:

- **Issuing a National Security Presidential Directive (NSPD) or Homeland Security Presidential Directive (HSPD) creating a "National Security Risk Management Program".** The HSPD/NSPD should establish a national program for security risk management, complete with funding for a system of governance of Federal efforts to produce a government-wide approach. Through such a program, the White House could accelerate progress, reduce massive duplication of efforts, and eliminate organizational conflicts and other barriers.

- **Creating a security risk analysis governance infrastructure to help bring rigor and standardization to the assessment of security risks, while increasing confidence in the outcome.** To this end, the creation of the following two organizations is recommended:

[2] U.S. Government Accountability Office, Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure, GAO-06-91, Dec. 2005, available at [http://www.gao.gov/new.items/d0691.pdf] accessed Sep. 25, 2007

[3] Congressional Research Service, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress, Order Code RL33858, Feb. 2, 2007, available at http://www.fas.org/sgp/crs/homesec/RL33858.pdf, accessed Sept.25, 2007

- ***A Security Advisory and Risk Standards Board (SARSB).*** A SARSB would be officially recognized as the authoritative body for Federal security risk management strategy, policy and standards. Similar in concept to the approach used by the Financial Accounting Standards Board (FASB) in establishing Generally Accepted Accounting Principles (GAAP) for the accounting industry, it would provide oversight, guidance and standards development for all Federal agencies. The leadership of the SARSB should include representatives from all agencies with significant homeland security and national security responsibilities.

  The role of the SARSAB would be to:

  - Develop a national architecture for Federal security risk management and work in partnership with state and local government, the private sector, professional associations and academia to translate the architecture into a roadmap for implementation.

  - Be the Government's authority on security risk management, with responsibility for developing voluntary consensus standards and recognizing best practices.

  - Advise all Federal departments and agencies on the development of new risk assessment methodologies, programs and policies, and promote the convergence of existing approaches toward more unified and compatible methods.

  - Specify national level requirements for intelligence and counter-intelligence information needed to support the threat analyses to be used in risk assessments.

  - Provide an annual report card on the progress of individual Federal agencies in implementing risk management programs to support security decision-making and investment prioritization.

  - On an as-needed basis, chair dispute resolution meetings with Federal departments or agencies with disagreements over security risk management activities and policies that may affect national/homeland security interests.

- ***An Interagency Risk Management Support Staff*** **(IRMSS).** The function of an IRMSS would be to provide program development support, technical expertise and training to Federal, state and local governments, as well as the private sector. Addressing the shortage of qualified risk methodologists and trainers in the Federal Government, the IRMSS mission would centralize that expertise, making it available in one place to support practitioners in achieving the national goal of a mature, unified and broadly-accepted approach. It is also possible that such a mission could be delegated to an existing organization, such as the Interagency OPSEC Support Staff, which has deep experience in supporting the national OPSEC Program at an interagency level.

The role of the IRMSS would be to:

- Support the National Risk Management Program by providing tailored training and assisting in program development.
- Produce educational multimedia products and presenting at conferences for the homeland security, defense, intelligence and public safety communities.
- Help Federal, state and local government organizations develop self-sufficient interoperable risk management programs in order to protect the American public, infrastructure and activities.

Guidance

Through the aforementioned approach, the White House could direct:

- **Federal departments and agencies to create a Chief Risk Officer (CRO) position to synchronize, coordinate and monitor all security risk efforts within their organizations.** The CRO concept has been in widespread use by the private sector for decades. Implementing such a position within key Federal departments and agencies would elevate the importance of risk management and end debates over who creates the necessary policies and procedures and leads the risk management initiatives at the department and/or agency-level.
- **Mandate that Federal departments and agencies participate in resolving their differences through the SARSB.** Participation in a respected, non-governmental body, such as the SARSB, would help to elevate the discussion beyond the unique and sometimes parochial interests of Federal departments and agencies that have often doomed previous attempts to improve the uniformity of risk management methods.

Public-Private Partnerships

Any comprehensive solution must also include active partnerships with the security industry as an integral partner in achieving national plans, such as the National Infrastructure Protection Plan (NIPP). Therefore, the White House should consider recognizing appropriate security analysis/risk management professional associations as partners in representing the private sector, academia and the security risk analysis profession at large. Federal departments and agencies should seek to benefit from the deeper and broader experience available through such associations. The creation of this public-private partnership is necessary to establish communication and buy-in between Federal and private sector practitioners engaged in supporting national and homeland security missions. Such participation will allow for the broadest input and greatly facilitate the adoption of standards by the private sector. In turn, this will lead to a more uniform implementation of security risk management in the United States.

SARMA is one such association working to address many of the necessary foundational elements through its Common Knowledge Base (CKB) Program. The initial focus of CKB Program is threefold: 1) documenting the analytical methods

already in use; 2) establishing a common lexicon for security risk analysis; and, 3) developing standardized approaches to key security risk analysis issues. To that end, three specific projects have thus far been initiated:

- The **Common Lexicon Project** is focusing on developing a broad-based, consensus solution to the "language barrier" through the orderly collection of existing terms, linguistic deconstruction of definitions, and the application of a consensus process to arrive at acceptable common definitions.

- The **Encyclopedia of Security Analysis and Risk Assessment Methods** is using a Wiki-based approach to allow security practitioners across the nation to provide documented descriptions of their methodologies in a current "state of the profession" virtual encyclopedia.

- The **Generally Accepted Risk Assessment Principles Project**, or GARAP, is identifying and promulgating common practices and generally accepted principles to bring added rigor and standardization to the process of assessing security risks.

Each of these projects is being implemented in an open and transparent manner to encourage participation by the broadest possible range of security risk analysis practitioners. To learn more, visit the SARMA CKB Program web site at: http://sarma-wiki.org.

Conclusions

The terrorist attacks of September 11, 2001, highlighted the difficulty of protecting an almost infinite number of targets with finite resources. The use of security risk management is the approach chosen by our Nation's leadership to address this problem. Yet, in order to ensure the effectiveness of this effort and accurately quantify its impact, the development and implementation of a national strategy for security risk management is needed. The refinement and application of a more uniform and coordinated approach to analyzing security risks will greatly enhance our Nation's ability to understand and manage a multitude of risks. It will also lead to improved decision-making by Congress and the White House, as well as more efficient prioritization of resources.

The creation of such a national system of governance and standards for security risk management is beyond the mission and authorities of any one Federal department or agency. Even with visionary leadership and direction it will not be easy, as the U.S. Government Accountability Office and others have noted. Yet such a system is necessary if we are to protect the people, infrastructure and economic prosperity of the United States. The authors encourage the White House, Congress, Federal departments and agencies, State and local governments and the security profession to join forces and strive to achieve a National security risk management program that will help provide the Nation the security it needs at a price it can afford.

About the Authors

Edward J. Jopeck

Ed Jopeck is a Senior Principal at SRA International specializing in security analysis, risk assessment, risk management, intelligence and infrastructure protection. Over his 20-year career in the field he has developed, evaluated and applied security risk assessment methodologies in the intelligence, defence and homeland security communities. Between 2003 and 2007 he served as a security risk management consultant to the US Department of Homeland Security, where he led the development of strategic-level antiterrorism risk analysis methods and initiatives. He has also led antiterrorism risk assessments of large U.S. water supply systems serving nearly 12 million people, and assessed 19 federally-owned high-hazard dams, and associated hydropower plants.

Prior to September 11, 2001, Mr. Jopeck worked as an intelligence and security analyst for the Central Intelligence Agency, and later as a security analysis and risk management consultant to numerous other governmental organizations. While at CIA, Mr. Jopeck was a key developer and lead instructor of the CIA's Analytical Risk Management training program which was awarded a National Intelligence Meritorious Unit Citation by the Director of Central Intelligence.

Mr Jopeck is currently serving his second term as the Founding President and Chairman of the Board of the Security Analysis and Risk Management Association (SARMA), a professional association working to mature security risk management practices and advance the profession of security analysis.

Kerry L. Thomas

Kerry Thomas recently joined the Washington Federal Practice (WFP) of PricewaterhouseCoopers (PwC) after more than ten years of Federal service. Mr. Thomas is currently overseeing the development of PWC's enterprise risk management solution for government agencies, as well as working to develop a suite of grant-related services for Federal clients. His work also includes advising various government and private sector clients on homeland security, risk management and grant-related matters.

Mr. Thomas previously served as a senior official within the U.S. Department of Homeland Security where he was responsible for the development of policy, as well as oversight and management of a broad range of grants, technical assistance programs, risk assessments and other services for the protection of critical infrastructure and key resources.

Mr. Thomas is also currently serving as the Executive Vice President of the Security Analysis and Risk Management Association (SARMA), and as a member of the SARMA Board of Directors. He has a Masters Degree in Public Management from the University of Maryland in College Park, Maryland, and a Bachelors Degree in Political Science from Texas Christian University in Fort Worth, Texas. A native of Texas, Mr. Thomas has resided in the Washington, D.C. area since 1993.